CYCLES OF RANDOM PERMUTATIONS WITH RESTRICTED CYCLE LENGTHS

FLORENT BENAYCH-GEORGES

Abstract. We prove some general results about the asymptotics of the distribution of the number of cycles of given length of a random permutation whose distribution is invariant under conjugation. These results were first established to be applied in a forthcoming paper [BG], where we prove results about cycles of random permutations which can be written as free words in several independent random permutations. However, we also apply them here to prove asymptotic results about random permutations with restricted cycle lengths. More specifically, for A a set of positive integers, we consider a random permutation chosen uniformly among the permutations of $\{1,\dots,n\}$ which have all their cycle lengths in A, and then let n tend to infinity. Improving slightly a recent result of Yakymiv [Y07], we prove that under a general hypothesis on A, the numbers of cycles with fixed lengths of this random permutation are asymptotically independent and distributed according to Poisson distributions. In the case where A is finite, we prove that the behavior of these random variables is completely different: cycles with length $\max A$ are predominant.

Introduction

It is well known that if for all positive integers n, σ_n is a random permutation chosen uniformly among all permutations of $\{1,\dots,n\}$ and if for all positive integers l, $N_l(\sigma_n)$ denotes the number of cycles of length l in the decomposition of σ_n as a product of cycles with disjoint supports, then for all $l\geq 1$, the joint distribution of the random vector

$$(N_1(\sigma_n),\dots,N_l(\sigma_n))$$

converges weakly, as n goes to infinity, to

$$\mathrm{Poiss}(1/1)\otimes\mathrm{Poiss}(1/2)\otimes\cdots\otimes\mathrm{Poiss}(1/l),$$

where for all positive number λ, $\mathrm{Poiss}(\lambda)$ denotes the Poisson distribution with mean λ.

The proof of this result is rather simple (see, e.g. [DS94, ABT05]) because the uniform distribution on the symmetric group is easy to handle. However, many other distributions on the symmetric group give rise to limit distributions for "small cycles", i.e. for the number of cycles of given length. In the first section of this paper, we shall prove a general theorem about the convergence of the distributions of the number of cycles of given length of random permutations distributed according to measures which are invariant under conjugation (Theorem 1.1). This result plays a key role in a forthcoming paper [BG], were we prove results about cycles of random permutations which can be written as free words in several independent random

Date: January 16, 2009.
MSC 2000 subject classifications. primary 20B30, 60B15, secondary 60C05.
Key words. Random permutations, cycles of random permutations, random permutations with restricted cycle lengths, A-permutations.

permutations with restricted cycle length. More precisely, in [BG], Corollary 3.2 (thus also, indirectly, Theorems 3.7 and 3.8) and Theorem 3.12 are consequences of Theorem 1.1 or of Corollary 1.3 of the present paper.

In the second part of the paper, for A set of positive integers, we introduce $\mathfrak{S}_n^{(A)}$ to be the set of permutations of $\{1, \ldots, n\}$ which have all their cycle lengths in A (such permutations are sometimes called A-*permutations*). For all n such that $\mathfrak{S}_n^{(A)}$ is nonempty, we consider a random permutation σ_n chosen uniformly in $\mathfrak{S}_n^{(A)}$.

We first prove, as an application of our general result mentioned above, that under certain hypothesis on an infinite set A, the result presented in the first paragraph about uniform random permutations stays as true as it can (as long as we consider the fact that for all $l \notin A$, $N_l(\sigma_n)$ is almost surely null): for all $l \geq 1$, the distribution of the random vector

$$(N_k(\sigma_n))_{1 \leq k \leq l, k \in A} \tag{1}$$

converges weakly, as n goes to infinity in such a way that $\mathfrak{S}_n^{(A)}$ is non empty, to

$$\bigotimes_{1 \leq k \leq l, k \in A} \operatorname{Poiss}(1/k). \tag{2}$$

Here, we shall mention that as the author published this work on arxiv, it was pointed out to him that proving this result under some slightly stronger hypothesis was exactly the purpose of a very recent paper [Y07]. However, the method used in this article is different from the one we use here: it relies on an identity in law between the random vector of (1) and a vector with law (2) conditioned to belong to a certain set and on some estimations provided by asymptotic behavior of generating functions. It is the approach of analytic combinatorics, which provides a powerful machinery for the analysis of random combinatorial objects. The book [FS08] offers synthetic presentation of these tools. It is possible that the result presented in this paragraph can be deduced from chapter IX of this book, but our proof is very short, and the object of the present paper is overall to prove the general result presented above about random permutations whose distributions are invariant under conjugation.

Note that the result presented in the previous paragraph implies that the number of cycles of any given length "stays finite" even though n goes to infinity, i.e. takes large values with a very small probability. Hence if A is finite, such a result cannot be expected. We also study this case here, and prove that if one denotes $\max A$ by d, for all $l \in A$, $N_l(\sigma_n)/n^{l/d}$ converges in every L^p space to $1/l$. As a consequence, the cycles with length d will be predominant: the cardinality of the subset of $\{1, \ldots, n\}$ covered by the supports of cycles with length d in such a random permutation is asymptotic to n, which means that the random permutation is not far away from having order d. This remark will appear to be very helpful in the study of words in independent such random permutations.

Notation. In this text, we shall denote by $\mathbb{N}$ the set of nonnegative integers,. For n an integer, we shall denote $\{1, \ldots, n\}$ by $[n]$ and the group of permutations of $[n]$ by $\mathfrak{S}_n$. For A set of positive integers, $\mathfrak{S}_n^{(A)}$ denotes the set of permutations of $[n]$, all of whose cycles have length in A. For $\sigma \in \mathfrak{S}_n$ and l a positive integer, we shall denote by $N_l(\sigma)$ the number of cycles of length l in the decomposition of σ as a product of cycles with disjoint supports. For $\lambda > 0$, $\operatorname{Poiss}(\lambda)$ will denote the Poisson distribution with parameter λ. If I is a set, $|I|$ shall denote its cardinality.

Acknowledgments. The author would like to thank Professor Vatutin for having mentioned

to him the works of Yakymiv and Pavlov, and Professor Yakymiv for his support and some interesting remarks about a draft of this work. He also would like to thank an anonymous referee for many interesting suggestions.

1. A general result about cycles of random permutations

1.1. **Main results.** The main results of this section are Theorem 1.1 and Corollary 1.3. Both of them play a key role in the paper [BG]. Recall that for all n integer, a probability measure $\mathbb{P}$ on $\mathfrak{S}_n$ is said to be *invariant under conjugation* if for all $\sigma, \tau \in \mathfrak{S}_n$, $\mathbb{P}(\{\sigma \circ \tau \circ \sigma^{-1}\}) = \mathbb{P}(\{\tau\})$.

Theorem 1.1. *Let $\mathcal{N}$ be an infinite set of positive integers. Fix a positive integer q, some positive integers $l_1 < \cdots < l_q$ and some probability measures $\mu_1, \ldots, \mu_q$ on the set of positive integers. Let, for for each $n \in A$, $\mathbb{P}_n$ be probability measure on $\mathfrak{S}_n$ which is invariant under conjugation. Suppose that for all $p \geq 1$, for all $k = (k_1, \ldots, k_q) \in \mathbb{N}^q$ such that $k_1 l_1 + \cdots + k_q l_q = p$ and for all $\sigma \in \mathfrak{S}_p$ which has k_1 cycles of length l_1, ..., k_q cycles of length l_q, the sequence*

$$\frac{n^p}{l_1^{k_1} \cdots l_q^{k_q} k_1! \cdots k_q!} \mathbb{P}_n(\{\tau \in \mathfrak{S}_n\,;\, \forall i = 1, \ldots, p, \tau(i) = \sigma(i)\})$$

converges, as $n \in \mathcal{N}$ tends to infinity, to a limit, denoted by S_k, such that for all $r_1, \ldots, r_q \geq 0$, we have

$$\sum_{k_1 \geq r_1} \cdots \sum_{k_q \geq r_q} (-1)^{k_1 - r_1 + \cdots + k_q - r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} S_{(k_1, \ldots, k_q)} = \prod_{1 \leq i \leq q} \mu_i(r_i). \tag{3}$$

Then, if, for all $n \in \mathcal{N}$, σ_n is a random variable distributed according to $\mathbb{P}_n$, the law of $(N_{l_1}(\sigma_n), \ldots, N_{l_q}(\sigma_n))$ converges, as $n \in \mathcal{N}$ tends to infinity, to $\mu_1 \otimes \cdots \otimes \mu_q$.

Remark 1.2. *Note that the series of (3) are not asked to converge absolutely. We only ask the sequence*

$$\sum_{\substack{k_1 \geq r_1, \ldots, k_q \geq r_q \\ k_1 - r_1 + \cdots + k_q - r_q \leq n}} (-1)^{k_1 - r_1 + \cdots + k_q - r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} S_{(k_1, \ldots, k_q)},$$

to tend to the right hand term of (3) as n tends to infinity.

Theorem 1.1 will be proved in Section 1.3. Let us now give its main corollary.

Corollary 1.3. *Let $\mathcal{N}$ be an infinite set of positive integers. Let A be a set of positive integers and let, for each $n \in \mathcal{N}$, σ_n be a random element of $\mathfrak{S}_n$, distributed according to a probability measure which is invariant under conjugation. Suppose that for all $p \geq 1$, for all $\sigma \in \mathfrak{S}_p^{(A)}$, the probability of the event*

$$\{\forall m = 1, \ldots, p, \sigma_n(m) = \sigma(m)\}$$

is asymptotic to n^{-p} as $n \in \mathcal{N}$ goes to infinity. Then for any finite subset K of A, the law of $(N_l(\sigma_n))_{l \in K}$ converges, as $n \in \mathcal{N}$ goes to infinity, to $\bigotimes_{l \in K} \mathrm{Poiss}(1/l)$.

Remark 1.4. *Note that the reciprocal implication is false. Consider for example a random permutation σ_n with law $\left(1 - \frac{1}{n}\right)\mathcal{U} + \frac{1}{n}\delta_{Id}$, where $\mathcal{U}$ denotes the uniform law on $\mathfrak{S}_n$. Then the probability of the event $\{\sigma_n(1) = 1\}$ is asymptotic to $2/n$ as n tends to infinity.*

Proof of Corollary 1.3. The proof is immediate, since clearly, if one fixes a finite family $l_1 < \cdots < l_q$ of elements of A, then Theorem 1.1 can be applied with $\mathbb{P}_n = \mathrm{Law}(\sigma_n)$ for all n, with $\mu_1 = \mathrm{Poiss}(1/l_1), \ldots, \mu_q = \mathrm{Poiss}(1/l_q)$ and with the S_k's given by

$$\forall k_1, \ldots, k_q, \quad S_{(k_1,\ldots,k_q)} = \frac{1}{l_1^{k_1} \cdots l_q^{k_q} k_1! \cdots k_q!}.$$

□

1.2. **Technical preliminaries to the proof of Theorem 1.1.** Before the proof of Theorem 1.1, we shall prove Proposition 1.6, which is a kind of Bonferroni inequality for inclusion-exclusion. The principle is not new, but we did not find this result in the literature.

Let us first recall Theorem 1.8 of [B01].

Theorem 1.5. *Fix $n, N \geq 1$, $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$, $I_1, J_1, \ldots, I_n, J_n$ subsets of $[N]$. Then in order to have*

$$\sum_{k=1}^{n} \lambda_k \, \mathbb{P}((\cap_{i \in I_i} A_i) \cap (\cap_{i \in J_i} (\Omega \backslash A_i))) \geq 0$$

for any family $A_1, \ldots, A_N$ of events in any probability space $(\Omega, \Sigma, \mathbb{P})$, it suffices to prove it under the additional hypothesis that each of the A_i's is either $\emptyset$ or Ω.

Proposition 1.6. *Consider a probability space $(\Omega, \Sigma, \mathbb{P})$, $q \geq 1$, finite sets $I_1, \ldots, I_q$ and, for all $i = 1, \ldots, q$, $(A_{i,j})_{j \in I_i}$ a finite family of events of Σ. Let us define the random vector $C = (C_1, \ldots, C_q)$ by, for $i = 1, \ldots, q$ and $\omega \in \Omega$,*

$$C_i(\omega) = |\{j \in I_i \, ; \, \omega \in A_{i,j}\}|.$$

Let us also define, for $k = (k_1, \ldots, k_q) \in \mathbb{N}^q \backslash \{0\}$,

$$S_k = \sum_{\substack{J_1 \subset I_1 \\ |J_1| = k_1}} \cdots \sum_{\substack{J_q \subset I_q \\ |J_q| = k_q}} \mathbb{P}(\cap_{l=1}^{q} \cap_{j \in J_l} A_{i,j})$$

and $S_0 = 1$. Then for all $r = (r_1, \ldots, r_q) \in \mathbb{N}^q$,

$$\mathbb{P}(C = r) = \sum_{k_1 = r_1}^{|I_1|} \cdots \sum_{k_q = r_q}^{|I_q|} (-1)^{k_1 - r_1 + \cdots + k_q - r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} S_{(k_1,\ldots,k_q)}. \tag{4}$$

Moreover, alternating inequalities of the following type are satisfied: for all $m \geq 0$ odd (resp. even),

$$\mathbb{P}(C = r) \geq \sum (-1)^{k_1 - r_1 + \cdots + k_q - r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} S_{(k_1,\ldots,k_q)} \qquad (\textit{resp. } \leq), \tag{5}$$

where the sum runs over all families $(k_1, \ldots, k_q)$ of nonnegative integers such that $r_1 \leq k_1 \leq |I_1|$, $\ldots$, $r_q \leq k_q \leq |I_q|$ and $k_1 - r_1 + \cdots + k_q - r_q \leq m$.

Proof. Firstly, note that the alternating inequalities, used for m large enough, imply (4). So we are only going to prove the alternating inequalities.

One can suppose that for each $i = 1, \ldots, q$, $I_i = [n_i]$, with n_i a positive integer. As an application of the previous theorem, one can suppose every $A_{i,j}$ to be either $\emptyset$ or Ω. In this case,

for all $i = 1, \dots, q$, the random variable C_i is constant, equal to the number c_i of j's such that $A_{i,j} = \Omega$, and for all $k = (k_1, \dots, k_q) \in \mathbb{N}^q$,

$$S_k = \binom{c_1}{k_1} \cdots \binom{c_q}{k_q}.$$

Hence for $(r_1, \dots, r_q) = (c_1, \dots, c_q)$, for all $m \geq 0$,

$$\begin{aligned}
&\sum_{\substack{k_1=r_1,\dots,n_1\\ \vdots \\ k_q=r_q,\dots,n_q\\ k_1-r_1+\cdots+k_q-r_q\leq m}} (-1)^{k_1-r_1+\cdots+k_q-r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} S_{(k_1,\dots,k_q)} \\
&= \sum_{\substack{k_1=c_1,\dots,n_1\\ \vdots \\ k_q=c_q,\dots,n_q\\ k_1-r_1+\cdots+k_q-r_q\leq m}} (-1)^{k_1-r_1+\cdots+k_q-r_q} \binom{k_1}{c_1} \cdots \binom{k_q}{c_q} \binom{c_1}{k_1} \cdots \binom{c_q}{k_q},
\end{aligned}$$

which is equal to 1, i.e. to $\mathbb{P}(C = r)$.

Now, consider $(r_1, \dots, r_q) \neq (c_1, \dots, c_q)$. Then $\mathbb{P}(C = r) = 0$ and we have to prove that the right-hand-side term in equation (5) is either nonnegative or nonpositive according to whether m is even or odd. For all $m \geq 0$,

$$\begin{aligned}
&\sum_{\substack{k_1=r_1,\dots,n_1\\ \vdots \\ k_q=r_q,\dots,n_q\\ k_1-r_1+\cdots+k_q-r_q\leq m}} (-1)^{k_1-r_1+\cdots+k_q-r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} S_{(k_1,\dots,k_q)} \\
&= \sum_{\substack{k_1=r_1,\dots,n_1\\ \vdots \\ k_q=r_q,\dots,n_q\\ k_1-r_1+\cdots+k_q-r_q\leq m}} (-1)^{k_1-r_1+\cdots+k_q-r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} \binom{c_1}{k_1} \cdots \binom{c_q}{k_q} \\
&= \sum_{\substack{k_1=r_1,\dots,c_1\\ \vdots \\ k_q=r_q,\dots,c_q\\ k_1-r_1+\cdots+k_q-r_q\leq m}} (-1)^{k_1-r_1+\cdots+k_q-r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} \binom{c_1}{k_1} \cdots \binom{c_q}{k_q}.
\end{aligned}$$

If there exists i such that $r_i > c_i$, then the previous sum is zero. In the other case, since for all $0 \leq r \leq k \leq c$, $\binom{k}{r}\binom{c}{k} = \binom{c}{r}\binom{c-r}{l}$ for $l = k - r$, the previous sum is equal to

$$\binom{c_1}{r_1} \cdots \binom{c_q}{r_q} \sum_{\substack{l_1=0,\dots,c_1-r_1\\ \vdots \\ l_q=0,\dots,c_q-r_q\\ l_1+\cdots+l_q\leq m}} (-1)^{l_1+\cdots+l_q} \binom{c_1-r_1}{l_1} \cdots \binom{c_q-r_q}{l_q}.$$

So we have to prove that for all $d=(d_1,\dots,d_q)\in\mathbb{N}^q\backslash\{0\}$ and for all $m\in\mathbb{N}$,

$$Z(m,d):=(-1)^m\sum_{\substack{l_1=0,\dots,d_1\\ \vdots\\ l_q=0,\dots,d_q\\ l_1+\cdots+l_q\le m}}(-1)^{l_1+\cdots+l_q}\binom{d_1}{l_1}\cdots\binom{d_q}{l_q}$$

is nonnegative. Let us prove it by induction over $d_1+\cdots+d_q\ge 1$.

If $d_1+\cdots+d_q=1$, then

$$Z(m,d)=\begin{cases}1 & \text{if } m=0,\\ 0 & \text{if } m>0,\end{cases}$$

so the result holds.

Suppose the result to be proved to the rank $d_1+\cdots+d_q-1\ge 1$. First note that if $m=0$, then $Z(m,d)=1$, so the result holds. So let us suppose that $m\ge 1$. Since $d_1+\cdots+d_q\ge 2$, there exists i_0 such that $d_{i_0}\neq 0$. One can suppose that $i_0=q$. Using $\binom{d_q}{l_q}=\binom{d_q-1}{l_q}+\binom{d_q-1}{l_q-1}$, one has

$$Z(m,d)=Z(m,(d_1,\dots,d_{q-1},d_q-1))+Z(m-1,(d_1,\dots,d_{q-1},d_q-1)),$$

which completes the proof of the induction, and of the proposition. □

1.3. **Proof of Theorem 1.1.** Before the beginning of the proof, let us introduce some notation. Let $\mathfrak{C}_l(n)$ be the set of cycles of $[n]$ with length l. Let, for all cycle c of $[n]$,

$$E_c(n)=\{\sigma\in\mathfrak{S}_n\,;\,c\text{ appears in the cycle decomposition of }\sigma\}.$$

Step I. In order to prove the theorem, we fix a family of nonnegative integers $(r_1,\dots,r_q)$, and we prove that the probability of the event

$$\{\forall i=1,\dots,q,N_{l_i}(\sigma_n)=r_i\}$$

converges, as n goes to infinity, to

$$\prod_{1\le i\le q}\mu_i(r_i),$$

i.e. to

$$\sum_{k_1\ge r_1}\cdots\sum_{k_q\ge r_q}(-1)^{k_1-r_1+\cdots+k_q-r_q}\binom{k_1}{r_1}\cdots\binom{k_q}{r_q}S_{(k_1,\dots,k_q)}. \tag{6}$$

With the notations introduced above, we have to prove that

$$\mathbb{P}_n(\forall i=1,\dots,q,\ \text{exactly } r_i \text{ of the events of the family } (E_c(n))_{c\in\mathfrak{C}_{l_i}(n)} \text{ occur}) \tag{7}$$

converges, as n goes to infinity, to (6).

By (4), for all n, the probability of (7) is

$$\sum_{k_1=r_1,\dots,|\mathfrak{C}_{l_1}(n)|}\cdots\sum_{k_q=r_q,\dots,|\mathfrak{C}_{l_q}(n)|}(-1)^{k_1-r_1+\cdots+k_q-r_q}\binom{k_1}{r_1}\cdots\binom{k_q}{r_q}S_{(k_1,\dots,k_q)}(n), \tag{8}$$

where we have defined $S_0(n)=1$ and for all $k=(k_1,\dots,k_q)\in\mathbb{N}^q\backslash\{0\}$,

$$S_k(n):=\sum\mathbb{P}_n(\bigcap_{i\in[q]}\bigcap_{c\in J_i}E_c(n)), \tag{9}$$

the sum running over all families $(J_i)_{i\in[q]}$ such that for all i, $J_i \subset \mathfrak{C}_{l_i}(n)$ and $|J_i| = k_i$.

Step II. Let us fix $k = (k_1, \dots, k_q) \in \mathbb{N}^q \backslash \{0\}$ and compute $\lim_{n\to\infty} S_k(n)$. Define $p = k_1 l_1 + \cdots + k_q l_q$ and consider $\sigma \in S_p$ such that the decomposition in cycles of σ contains k_1 cycles of length l_1, k_2 cycles of length l_2, …, k_q cycles of length l_q. Then the invariance of $\mathbb{P}_n$ by conjugation allows us to claim that $S_k(n)$ is equal to

$$\mathbb{P}_n(\{\sigma \in \mathfrak{S}_n \,;\, \forall i = 1, \dots, p, \sigma_n(i) = \sigma(i)\})$$

times the number of sets J of cycles of $[n]$ which consist exactly in k_1 cycles of length l_1, k_2 cycles of length l_2, …, k_q cycles of length l_q such that these cycles are pairwise disjoint. Such a set J is defined by a set of pairwise disjoint subsets of $[n]$, which consists exactly of k_1 subsets of cardinality l_1, k_2 subsets of cardinality l_2, …, k_q subsets of cardinality l_q, and for every of these subsets, by the choice of a cycle having the subset for support. Hence there are exactly

$$\underbrace{\frac{n!}{(n-p)!l_1!^{k_1} l_2!^{k_2} \cdots l_q!^{k_q}} \frac{1}{k_1!k_2!\cdots k_q!}}_{\text{counting the sets of pairwise disjoint subsets of } [n]} \underbrace{(l_1-1)!^{k_1}(l_2-1)!^{k_2}(l_3-1)!^{k_3}\cdots(l_q-1)!^{k_q}}_{\text{choice of the cycles}}$$

such sets J. So

$$S_k(n) = \frac{n!}{(n-p)! l_1^{k_1} l_2^{k_2} \cdots l_q^{k_q}} \frac{1}{k_1!k_2!\cdots k_q!} \mathbb{P}_n(\{\sigma \in \mathfrak{S}_n \,;\, \forall i = 1, \dots, p, \sigma_n(i) = \sigma(i)\}).$$

Hence by hypothesis,

$$\lim_{n\to\infty} S_k(n) = S_{(k_1,\dots,k_q)}.$$

Step III. Now, let us prove that the probability of the event of (7) converges to (6). Fix $\varepsilon > 0$. Choose $m_0 \geq 0$ such that for all $m \geq m_0$, the absolute value of

$$\sum_{\substack{k_1 \geq r_1 \\ \vdots \\ k_q \geq r_q \\ k_1 - r_1 + \cdots + k_q - r_q > m}} (-1)^{k_1 - r_1 + \cdots + k_q - r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} S_{(k_1,\dots,k_q)},$$

is less than $\varepsilon/2$.

By (5), for all $m, m' \geq m_0$ such that m is odd and m' is even, the probability of the event of (7) is bounded from below by

$$\sum_{\substack{k_1 = r_1, \dots, |C_1(n)| \\ \vdots \\ k_q = r_q, \dots, |C_q(n)| \\ k_1 - r_1 + \cdots + k_q - r_q \leq m}} (-1)^{r_1 + k_1 + \cdots + r_q + k_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} S_{(k_1,\dots,k_q)}(n)$$

and bounded from above by

$$\sum_{\substack{k_1 = r_1, \dots, |C_1(n)| \\ \vdots \\ k_q = r_q, \dots, |C_q(n)| \\ k_1 - r_1 + \cdots + k_q - r_q \leq m'}} (-1)^{k_1 - r_1 + \cdots + k_q - r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} S_{(k_1,\dots,k_q)}(n).$$

Hence for n large enough, the probability of the event of (7) is bounded from below by

$$-\varepsilon/2 + \sum_{\substack{k_1\geq r_1\\ \vdots \\ k_q\geq r_q\\ k_1-r_1+\cdots+k_q-r_q\leq m}} (-1)^{k_1-r_1+\cdots+k_q-r_q}\binom{k_1}{r_1}\cdots\binom{k_q}{r_q}S_{(k_1,\ldots,k_q)}$$

and bounded from above by

$$\varepsilon/2 + \sum_{\substack{k_1\geq r_1\\ \vdots \\ k_q\geq r_q\\ k_1-r_1+\cdots+k_q-r_q\leq m'}} (-1)^{k_1-r_1+\cdots+k_q-r_q}\binom{k_1}{r_1}\cdots\binom{k_q}{r_q}S_{(k_1,\ldots,k_q)},$$

hence is ε-close to the sum of (6). It completes the proof of the theorem. □

2. Cycles of random permutations with restricted cycle lengths

First of all, let us recall that for n large enough, $\mathfrak{S}_n^{(A)}$ is non empty if and only if n is divided by the greatest common divisor of A (see Lemma 2.3 of [Ne07] for example).

2.1. Case where A is infinite.

The following proposition is the analog of the result stated in the beginning of the introduction, in the case where the random permutation we consider is not anymore distributed uniformly on the symmetric group but on the set of permutations all of whose cycles lengths fall in A (note that in this case, for all $k \notin A$, $N_k(\sigma_n)$ is almost surely null).

Proposition 2.1. *Suppose that A is a set of positive integers such that, if one denotes by q the greatest common divisor of A and by u_n the quotient $\left|\mathfrak{S}_{qn}^{(A)}\right|/(qn)!$, one has*

$$\frac{u_n}{u_{n-1}} \underset{n\to\infty}{\longrightarrow} 1. \tag{10}$$

We consider, for n large enough, a random permutation σ_n which has the uniform distribution on $\mathfrak{S}_{qn}^{(A)}$. Then for all $l \geq 1$, the distribution of the random vector

$$(N_k(\sigma_n))_{1\leq k\leq l, k\in A}$$

converges weakly, as n goes to infinity, to

$$\bigotimes_{1\leq k\leq l, k\in A} \operatorname{Poiss}(1/k).$$

Note also that this result implies that for all l, even for large values of n, every $N_l(\sigma_n)$ takes large values with a very small probability.

Proof. By Corollary 1.3, it suffices to prove that for all $p \geq 1$, for all $\sigma \in \mathfrak{S}_p^{(A)}$, the probability of the event $\{\forall m = 1,\ldots,p, \sigma_n(m) = \sigma(m)\}$ is asymptotic to n^{-p} as n goes to infinity. This probability is equal to

$$\frac{\left|\{s \in \mathfrak{S}_{qn}^{(A)}\,;\, \forall m = 1,\ldots,p, s(m) = \sigma(m)\}\right|}{\left|\mathfrak{S}_{qn}^{(A)}\right|} = \frac{\left|\mathfrak{S}_{qn-p}^{(A)}\right|}{\left|\mathfrak{S}_{qn}^{(A)}\right|},$$

hence the proposition follows from (10). □

Remark 2.2. *1. This result improves Theorem 1 of* [Y07]*, which states the same result under the slightly stronger hypothesis that* (u_n) *is a sequence with regular variation with exponent in* $(-1, 0]$*. However, the author did not find any example where the hypothesis of this result are satisfied but the hypothesis of Theorem 1 of* [Y07] *are not.*
2. A number of examples of classes of sets A *satisfying the hypothesis of this proposition holds can be fund in the list of examples following Theorem 2 of* [Y05a]*. It holds for example if* $|A \cap [n]| / n \underset{n\to\infty}{\longrightarrow} 1$*. More details are given in Theorem 3.3.1 of the book* [Y05b].

2.2. Case where A is finite.

We are going to prove the following result:

Theorem 2.3. *Suppose that* A *is a finite set of positive integers, and denote its maximum by* d*. We consider, for all* n *such that* $\mathfrak{S}_n^{(A)}$ *is non empty, a random permutation* σ_n *which has the uniform distribution on* $\mathfrak{S}_n^{(A)}$*. Then for all* $l \in A$*, as* n *goes to infinity in such a way that* $\mathfrak{S}_n^{(A)}$ *is non empty,* $\frac{N_l(\sigma_n)}{n^{l/d}}$ *converges in all* L^p *spaces (*$p \in [1, +\infty)$*) to* $1/l$*.*

Remark 2.4. *It would be interesting to know if we have a dilation of the random variables of* $N_l(\sigma_n)/n^{l/d} - 1/l$ *which has a non degenerate weak limit as* n *goes to infinity. It seems possible that analytic combinatorics, as presented in* [FS08]*, could provide a way to answer this question.*

To prove this theorem, we shall need the following lemmas. Lemma 2.5 is well known (see, for instance, Theorem 3.53 of [B04]). Lemma 2.6 is Lemma 3.6 of [Ne07].

Lemma 2.5. *Let* p *be the greatest common divisor of* A*. Then for all complex number* z*, one has*

$$\sum_{n\geq 0} \frac{\left|\mathfrak{S}_{pn}^{(A)}\right|}{(pn)!} z^{pn} = \exp\left(\sum_{k\in A} \frac{z^k}{k}\right).$$

Lemma 2.6. *Let* B *be a finite set of positive integers. Let* $(c_j)_{j\in B}$ *be a finite family of positive numbers. Let* $\sum_{n\geq 1} b_n w^n$ *be the power expansion of* $\exp\left(\sum_{j\in B} c_j w^j\right)$*. Suppose that* $b_n > 0$ *for sufficiently large* n*. Then, as* n *goes to infinity,*

$$\frac{b_{n-1}}{b_n} \sim \left(\frac{n}{bc_b}\right)^{1/b},$$

with $b = \max B$*.*

Proof of the theorem. First note that by Hölder formula, it suffices to prove that for all p positive integer, the expectation of the $2p$-th power of

$$\frac{N_l(\sigma_n)}{n^{l/d}} - \frac{1}{l}$$

tends to zero as n goes to infinity. Hence by the binomial identity, it suffices to prove that for all $l \in A$, for all $m \geq 1$, the expectation of the m-th power of $N_l(\sigma_n)$ is asymptotic to $n^{ml/d}/l^m$ as n goes to infinity in such a way that $\mathfrak{S}_n^{(A)}$ is non empty.

One can suppose that for all such n, the probability space where σ_n is defined is $\mathfrak{S}_n^{(A)}$, endowed with the uniform probability measure $\mathbb{P}_n$. Let $\mathbb{E}_n$ denote the expectation with respect to $\mathbb{P}_n$.

So let us fix $l \in A$ and $m \geq 1$. Since $N_l(\sigma_n) = \frac{1}{l}\sum_{k=1}^{n} 1_{\{k \text{ belongs to a cycle of length } l\}}$, one has

$$\mathbb{E}_n[N_l(\sigma_n)^m] = \frac{1}{l^m} \sum_{\substack{m_1,\ldots,m_n \geq 0 \\ m_1+\cdots+m_n = m}} \binom{m}{m_1,\ldots,m_n} \mathbb{E}_n\left[\prod_{k=1}^{n} (1_{\{k \text{ belongs to a cycle of length } l\}})^{m_k}\right]$$

But $\mathbb{P}_n$ is invariant by conjugation, so for all $m_1,\ldots,m_n \geq 0$,

$$\mathbb{E}_n\left[\prod_{k=1}^{n} (1_{\{k \text{ belongs to a cycle of length } l\}})^{m_k}\right]$$

depends only on the number j of k's such that $m_k \neq 0$. So

$$\begin{aligned}
\mathbb{E}_n[N_l(\sigma_n)^m] &= \frac{1}{l^m}\sum_{j=1}^{m} \sum_{\substack{m_1,\ldots,m_n \geq 0 \\ |\{k\in[n]\,;\, m_k \neq 0\}| = j \\ m_1+\cdots+m_n = m}} \binom{m}{m_1,\ldots,m_n} \mathbb{P}_n\left(1,\ldots,j \text{ belong to cycles of length } l\right) \\
&= \frac{1}{l^m}\sum_{j=1}^{m}\left[\binom{n}{j}\mathbb{P}_n\left(1,\ldots,j \text{ belong to cycles of length } l\right) \sum_{\substack{m_1,\ldots,m_j \geq 1 \\ m_1+\ldots+m_j = m}} \binom{m}{m_1,\ldots,m_j}\right]. \qquad (11)
\end{aligned}$$

Now, let us fix $j \geq 1$ and let us denote by $\mathrm{P}(j)$ the set of partitions of $[j]$. We have

$$\begin{aligned}
&\mathbb{P}_n\left(1,\ldots,j \text{ belong to cycles of length } l\right) \\
&= \sum_{\pi \in \mathrm{P}(j)} \mathbb{P}_n(1,\ldots,j \text{ are in cycles of length } l \\
&\qquad\qquad \text{and } \forall i,i' \in [j],\ [i,i' \text{ belong to the same cycle}] \Leftrightarrow [i = i' \mod \pi]) \\
&= \sum_{\substack{\pi\in\mathrm{P}(j) \\ \pi = \{V_1,\ldots,V_{|\pi|}\}}} \binom{n-j}{l-|V_1|,\ldots,l-|V_{|\pi|}|,n-l|\pi|} ((l-1)!)^{|\pi|} \frac{\left|\mathfrak{S}_{n-l|\pi|}^{(A)}\right|}{\left|\mathfrak{S}_{n}^{(A)}\right|} \\
&= \sum_{\pi\in\mathrm{P}(j)} \frac{1}{n(n-1)\cdots(n-j+1)} \frac{\left|\mathfrak{S}_{n-l|\pi|}^{(A)}\right|/(n-l|\pi|)!}{\left|\mathfrak{S}_{n}^{(A)}\right|/n!} \prod_{V\in\pi}\frac{(l-1)!}{(l-|V|)!}. \qquad (12)
\end{aligned}$$

Let p be the greatest common divisor of A. We know [Ne07, Lem. 2.3] that for all positive integer n, $\mathfrak{S}_n^{(A)} \neq \emptyset \Longrightarrow p|n$, and that for sufficiently large n, the inverse implication is also true. Hence by Lemma 2.5, for $z \in \mathbb{C}$, one has

$$\sum_{n\geq 0} \frac{\left|\mathfrak{S}_{pn}^{(A)}\right|}{(pn)!}(z^p)^n = \exp\left(\sum_{j\in\frac{1}{p}\cdot A} \frac{(z^p)^j}{pj}\right).$$

Hence for $w \in \mathbb{C}$, one has

$$\sum_{n\geq 0} \frac{\left|\mathfrak{S}_{pn}^{(A)}\right|}{(pn)!}w^n = \exp\left(\sum_{j\in\frac{1}{p}\cdot A} \frac{w^j}{pj}\right).$$

So by Lemma 2.6, as n goes to infinity, one has

$$\frac{\left|\mathfrak{S}_{pn-p}^{(A)}\right|/(pn-p)!}{\left|\mathfrak{S}_{pn}^{(A)}\right|/(pn)!} \sim \left(\frac{n}{(d/p)1/d}\right)^{p/d} = (pn)^{p/d}$$

(note that in the case where the greatest common divisor of A is 1, this result can be deduced from the main theorem of [P95]). It follows, by induction on k, that, as n goes to infinity in such a way that p divides n, for any positive integer k divisible by p, we have

$$\frac{\left|\mathfrak{S}_{n-k}^{(A)}\right|/(n-k)!}{\left|\mathfrak{S}_{n}^{(A)}\right|/(n)!} \sim n^{k/d}.$$

Hence in (12), for each partition π, the term corresponding to π is asymptotic to

$$n^{l|\pi|/d-j}\prod_{V\in\pi}\frac{(l-1)!}{(l-|V|)!},$$

thus in (12), the leading term is the one of the singletons partition, and

$$\mathbb{P}_n\left(1,\dots,j \text{ belong to cycles of length } l\right) \sim n^{(l/d-1)j}. \tag{13}$$

Combining (11) and (13), one gets $\mathbb{E}_n[N_l(\sigma_n)^m] \sim \dfrac{n^{lm/d}}{l^m}$, which completes the proof of the theorem. □

References

[ABT05] Arratia, Richard; Barbour, A. D.; Tavaré, Simon *Logarithmic combinatorial structures: a probabilistic approach* EMS Monographs in Mathematics. European Mathematical Society (EMS), Zürich, 2003.

[BG] Benaych-Georges, Florent *Cycles of free words in several random permutations with restricted cycles lengths.* Submitted, available on `http://www.cmapx.polytechnique.fr/~benaych/`

[B01] Bollobás, B. *Random Graphs*, second edition. 2001.

[B04] Bóna, M. *Combinatorics of permutations*, Chapman & Hall/CRC, Boca Raton, FL, 2004

[DS94] Persi Diaconis, Mehrdad Shahshahani *On the Eigenvalues of Random Matrices*, Jour. Appl. Prob, Special 31A, 49-62. (1994)

[FS08] Flajolet, P, Sedgewick, *Analytic combinatorics*, Cambridge University Press, Coming soon, now available on the web.

[Ne07] Neagu, M. *Asymptotic freeness of random permutation matrices with restricted cycles lengths.* Indiana Univ. Math. J. 56 (2007) 2017 - 2049

[P95] Pavlov, A. I. *On the number of permutations with a finite set of cycle lengths.* (Russian) Trudy Mat. Inst. Steklov. 207 (1994), 256–267; translation in Proc. Steklov Inst. Math. 1995, no. 6 (207), 233–242

[Y05a] A. L. Yakymiv, *The distribution of lengths of the m-th maximal cycle in a random A permutation.* Translated from russian in Discrete Math. Appl. 15 (5), 527-546 (2005).

[Y05b] A. L. Yakymiv, *Probabilistic applications of Tauberian theorems.* Translated by Andrei V. Kolchin. (English) Modern Probability and Statistics. Leiden: VSP.

[Y07] A. L. Yakymiv, *Random A-Permutations: Convergence to a Poisson Process.* Translated from russian in Mathematical Notes, 2007, Vol. 81, No. 6, pp. 840-846.

Florent Benaych-Georges, LPMA, UPMC Univ Paris 6, Case courier 188, 4, Place Jussieu, 75252 Paris Cedex 05, France.

E-mail address: `florent.benaych@gmail.com`